MIKE DEWINE
★ OHIO ATTORNEY GENERAL ★

➢ CONFIDENTIALITY / SENSITIVE DATA AND INFORMATION USE POLICY

Effective Date: **January 15, 2016**

I. PURPOSE

The Ohio Attorney General's Office (AGO) takes seriously the protection of sensitive data and information. This policy provides the requirements for protecting the confidentiality of matters involving the AGO, and the privacy of people who have sensitive data and information in our databases, electronic and paper files, and other records. This policy is designed to avoid the accidental loss of data and information by AGO employees and to protect the confidentiality, integrity, and availability of all data and information transmitted, maintained, and utilized by AGO employees.

II. SCOPE

This policy applies to all full-time or part-time permanent, intermittent, or temporary employees (including interns and intermittent employees), contractors, and/or externs of the AGO, and all other users of AGO computer resources, regardless of whether such users are working from the office, home, or while on official travel status.

III. DEFINITIONS

A. Sensitive Data and Information includes, but is not limited to:

1. Attorney work product and attorney/client information only if designated as such by the supervising attorney;
2. Social Security Numbers;
3. Physical characteristics and other biometric information;
4. Tax information;
5. Copyrighted or trade secret information; and/or
6. Any information designated by statute or otherwise as confidential, protected, or sensitive, including:
   a) Confidential Personal Information (CPI): Confidential personal information is personal information maintained in a personal information system that falls within the scope of section 1347.15 of the Revised Code and that the AGO is prohibited from releasing under Ohio's public records law. The following sections have personal information systems that fall within the scope of R.C. 1347.15: Education, Collections Enforcement, and Crime Victims Services. Please refer to the AGO's Confidential Personal Information Access policy for more information.
   b) Electronically Protected Health Information (EPHI): EPHI refers to any protected health information as defined by the Health Insurance Portability and Accountability Act (HIPPA, 45 C.F.R. 160), that is transmitted electronically. Electronically protected health information is information, including, but not limited to, demographic data, that relates to:

i. The individual's past, present, or future physical or mental health or condition;
ii. The provision of health care to the individual, or
iii. The past, present, or future payment for the provision of health care to the individual, and that
iv. Identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.
v. Individually identifiable information includes many common identifiers (e.g. name, address, birth date, Social Security Number).

c) Student Education Records and Personally Identifiable Information: As defined by the Family Educational Rights and Privacy Act (FERPA) codified in 34 C.F.R. 99.3. Personally identifiable student information includes, but is not limited to:
   i. Student grades;
   ii. Social Security Numbers, and/or;
   iii. Any other information, if taken together, that could disclose the identity of a student.

d) Criminal Justice Information: As defined by the Criminal Justice Information Services Security Policy as codified in 28 C.F.R. 20. Criminal Justice Information includes but is not limited to:
   i. Biometric Data: data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data;
   ii. Identity History Data: textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual;
   iii. Biographic Data: information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case;
   iv. Property Data: information about vehicles and property associated with crime when accompanied by any personally identifiable information;
   v. Case/Incident History: information about the history of criminal incidents; and/or
   vi. Criminal History Record information: information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, information, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release. Criminal Justice Information includes. 28 CFR 20.3.